

Dirac's theorem for random graphs

Choongbum Lee *

Benny Sudakov †

Abstract

A classical theorem of Dirac from 1952 asserts that every graph on n vertices with minimum degree at least $\lceil n/2 \rceil$ is Hamiltonian. In this paper we extend this result to random graphs. Motivated by the study of resilience of random graph properties we prove that if $p \gg \log n/n$, then a.a.s. every subgraph of $G(n, p)$ with minimum degree at least $(1/2 + o(1))np$ is Hamiltonian. Our result improves on previously known bounds, and answers an open problem of Sudakov and Vu. Both, the range of edge probability p and the value of the constant $1/2$ are asymptotically best possible.

1 Introduction

A *Hamilton cycle* of a graph is a cycle which passes through every vertex of the graph exactly once, and a graph is *Hamiltonian* if it contains a Hamilton cycle. Hamiltonicity is one of the most central notions in graph theory, and has been intensively studied by numerous researchers. The problem of determining Hamiltonicity of a graph is one of the NP-complete problems that Karp listed in his seminal paper [18], and accordingly, one cannot hope for a simple classification of such graphs. Therefore it is important to find general sufficient conditions for Hamiltonicity and in the last 60 years many interesting results were obtained in this direction. One of the first results of this type is a classical theorem proved by Dirac [12] in 1952, which asserts that every graph on n vertices of minimum degree at least $\lceil n/2 \rceil$ is Hamiltonian.

In this paper, we study Hamiltonicity of random graphs. The model of random graphs we study is the binomial model $G(n, p)$ (also known as the Erdős-Renyi random graph), which denotes the probability space whose points are graphs with vertex set $[n] = \{1, \dots, n\}$ where each pair of vertices forms an edge randomly and independently with probability p . We say that $G(n, p)$ possesses a graph property \mathcal{P} *asymptotically almost surely*, or a.a.s. for brevity, if the probability that $G(n, p)$ possesses \mathcal{P} tends to 1 as n goes to infinity. The earlier results on Hamiltonicity of random graphs were proved by Pósa [25], and Korshunov [21]. Improving on these results, Bollobás [9], and Komlós and Szemerédi [20] proved that if $p \geq (\log n + \log \log n + \omega(n))/n$ for some function $\omega(n)$ that goes to infinity together with n , then $G(n, p)$ is a.a.s. Hamiltonian. The range of p cannot be improved, since if $p \leq (\log n + \log \log n - \omega(n))/n$, then $G(n, p)$ a.a.s. has a vertex of degree at most one.

*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: choongbum.lee@gmail.com. Research supported in part by a Samsung Scholarship.

†Department of Mathematics, UCLA, Los Angeles, CA 90095. Email: bsudakov@math.ucla.edu. Research supported in part by NSF grant DMS-1101185, NSF CAREER award DMS-0812005 and by USA-Israeli BSF grant.

Recently, in [27] the authors proposed to study Hamiltonicity of random graphs in more depth by measuring how strongly the random graphs possess this property. Let \mathcal{P} be a monotone increasing graph property. Define the *local resilience* of a graph G with respect to \mathcal{P} as the minimum number r such that by deleting at most r edges from each vertex of G , one can obtain a graph not having \mathcal{P} . Using this notion, one can state the aforementioned Dirac's theorem as " K_n has local resilience $\lfloor n/2 \rfloor$ with respect to Hamiltonicity". Sudakov and Vu [27] initiated the systematic study of resilience of random and pseudorandom graphs with respect to various properties, one of which is Hamiltonicity. In particular, they proved that if $p > \log^4 n/n$, then $G(n, p)$ a.a.s. has local resilience at least $(1/2 + o(1))np$ with respect to Hamiltonicity.

There are several other papers that studied local resilience of random graphs with respect to various properties. For example, Balogh, Csaba, and Samotij [3] studied the property of containing almost spanning trees of bounded degree, and Böttcher, Kohayakawa, and Taraz [8] studied the property of containing almost spanning subgraphs of bounded degree. There is also a similar concept called *global resilience*, where one measures the total number of edges that needs to be removed in order to obtain a graph without the given property. Global resilience of random graphs has also been studied for many properties; in fact, some results in this direction were obtained even before the concept has been first formalized in [27]. Haxell, Kohayakawa, and Łuczak [14, 15] studied it with respect to the property of containing a fixed length cycle, Dellamonica, Kohayakawa, Marciniszyn, and Steger [11] studied it with respect to the property of containing long cycles, and Alon and Sudakov [2] studied it with respect to increasing the chromatic number. Recently, Conlon and Gowers [10], and Schacht [26] independently obtained a breakthrough result which resolves several open problems in this area, one of which establishes the global resilience of random graphs with respect to containing fixed subgraphs. For other recent results on resilience, see [2, 4, 5, 16, 19, 22, 23].

The above mentioned result of Sudakov and Vu can be viewed as a generalization of Dirac's Theorem, since a complete graph is also a random graph $G(n, p)$ with $p = 1$. This connection is very natural and in fact most of the resilience results can be viewed as a generalization of some classic graph theory result to random and pseudorandom graphs. Note that, the constant $1/2$ in the resilience bound for Hamiltonicity cannot be further improved. To see this, consider a partition of the vertex set of a random graph into two parts of size $n/2$ and remove all the edges between these parts. Since the graph is random this removes roughly half of the edges incident with each vertex and makes the graph disconnected. However, things become unclear when one considers the range of p . Recall that Bollobás, and Komlós and Szemerédi's result mentioned above implies that if $p > C \log n/n$ for some $C > 1$, then $G(n, p)$ is a.a.s. Hamiltonian. Therefore it is natural to believe, as was conjectured in [27], that $G(n, p)$ has local resilience $(1/2 + o(1))np$ with respect to Hamiltonicity already when $p \gg \log n/n$.

In addition to [27], several other results have been obtained on this problem. Frieze and Krivelevich [13] proved that there exist constants C and ε such that if $p \geq C \log n/n$, then $G(n, p)$ a.a.s. has local resilience at least εnp with respect to Hamiltonicity. This result was improved by Ben-Shimon, Krivelevich, and Sudakov [6] who showed that for all ε , there exists a constant C , such that if $p \geq C \log n/n$, then $G(n, p)$ has local resilience at least $(1/6 - \varepsilon)np$. In their recent paper [7], the same authors further improved this bound to $(1/3 - \varepsilon)np$. Our main theorem completely solves the resilience problem of Sudakov and Vu.

Theorem 1.1. *For every positive ε , there exists a constant $C = C(\varepsilon)$ such that for $p \geq \frac{C \log n}{n}$, a.a.s. every subgraph of $G(n, p)$ with minimum degree at least $(1/2 + \varepsilon)np$ is Hamiltonian.*

As mentioned above, the constant $1/2$ and the range of edge probability p are both asymptotically best possible.

Notation. A graph $G = (V, E)$ is given by a pair of its vertex set $V = V(G)$ and edge set $E = E(G)$. We sometimes use $|G|$ to denote the order of the graph. For a subset X of vertices, we use $e(X)$ to denote the number of edges within X , and for two sets X, Y , we use $e(X, Y)$ to denote the number of edges $\{x, y\}$ such that $x \in X, y \in Y$ (note that $e(X, X) = 2e(X)$). We use $N(X)$ to denote the collection of vertices of $V \setminus X$ which are adjacent to some vertex of X . For two graphs G_1 and G_2 over the same vertex set V , we define their intersection as $G_1 \cap G_2 = (V, E(G_1) \cap E(G_2))$, their union as $G_1 \cup G_2 = (V, E(G_1) \cup E(G_2))$, and their difference as $G_1 \setminus G_2 = (V, E(G_1) \setminus E(G_2))$.

When there are several graphs under consideration, to avoid ambiguity, we use subscripts such as $N_G(X)$ to indicate the graph that we are currently interested in. We also use subscripts with asymptotic notations to indicate dependency. For example, Ω_ε will be used to indicate that the hidden constant depends on ε . To simplify the presentation, we often omit floor and ceiling signs whenever these are not crucial and make no attempts to optimize absolute constants involved. We also assume that the order n of all graphs tends to infinity and therefore is sufficiently large whenever necessary. All logarithms will be in base $e \approx 2.718$.

2 Properties of random graphs

In this section we develop some properties of random graphs. The following concentration result, Chernoff's bound (see, e.g., [1, Theorem A.1.12]), will be used to establish these properties.

Theorem 2.1. *Let ε be a positive constant. If X be a binomial random variable with parameters n and p , then*

$$\mathbb{P}(|X - np| \geq \varepsilon np) \leq e^{-\Omega_\varepsilon(np)}.$$

Also, for $\lambda \geq 3np$,

$$\mathbb{P}(X - np \geq \lambda) \leq e^{-\Omega(\lambda)}.$$

We also state another useful concentration result that we will use later (see, e.g., [17, Theorem 2.10]). Let A and A' be sets such that $A' \subseteq A$. Let B be a fixed size subset of A chosen uniformly at random. Then the distribution of the random variable $|B \cap A'|$ is called the *hypergeometric distribution*.

Theorem 2.2. *Let ε be a fixed positive constant and let X be a random variable with hypergeometric distribution. Then,*

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq \varepsilon \mathbb{E}[X]) \leq e^{-\Omega_\varepsilon(\mathbb{E}[X])}.$$

We first state two standard results on random graphs, which estimates the number of edges and the degree of vertices. We omit their proofs which consist of straightforward applications of Chernoff's inequality.

Proposition 2.3. *For every positive ε , there exists a constant C such that for $p \geq \frac{C \log n}{n}$, the random graph $G = G(n, p)$ a.a.s. has $e(G) = (1 + o(1)) \frac{n^2 p}{2}$ edges, and $\forall v \in V$, $(1 - \varepsilon)np \leq \deg(v) \leq (1 + \varepsilon)np$.*

Proposition 2.4. *Let $p \geq \log n/n$, and $\omega(n)$ be an arbitrary function which goes to infinity as n goes to infinity. Then in $G = G(n, p)$, a.a.s. for every two subsets of vertices X and Y ,*

$$e(X, Y) = |X||Y|p + o(|X||Y|p + \omega(n)n).$$

It is well-known that random graphs have certain expansion properties, and that these properties are very useful in proving Hamiltonicity. Next proposition shows that the expansion property still holds even after removing some of its edges. Similar lemmas appeared in [22, 27].

Proposition 2.5. *For every positive ε , there exists a constant C such that for $p \geq \frac{C \log n}{n}$, the random graph $G = G(n, p)$ a.a.s. has the following property. For every graph H of maximum degree at most $(\frac{1}{2} - 2\varepsilon)np$, the graph $G' = G - H$ satisfies the following:*

- (i) $\forall X \subseteq V$, $|X| \leq (\log n)^{-1/4}p^{-1}$, $|N_{G'}(X)| \geq (\frac{1}{2} + \varepsilon)|X|np$,
- (ii) $\forall X \subseteq V$, $n(\log n)^{-1/2} \leq |X| \leq \frac{\varepsilon}{2}n$, $|N_{G'}(X)| \geq (\frac{1}{2} + \varepsilon)n$, and
- (iii) G' is connected.

Proof. Let H be a graph of maximum degree at most $(\frac{1}{2} - 2\varepsilon)np$, and let $G' = G - H$.

(i) To prove (i), it suffices to prove that a.a.s. for all $X \subseteq V$ of size at most $(\log n)^{-1/4}p^{-1}$,

$$|N_G(X)| \geq (1 - \varepsilon)|X|np,$$

since it will imply by the maximum degree condition of H that

$$|N_{G'}(X)| \geq |N_G(X)| - \left(\frac{1}{2} - 2\varepsilon\right)np \cdot |X| \geq \left(\frac{1}{2} + \varepsilon\right)np \cdot |X|.$$

Fix a set $X \subseteq V$ of size $|X| \leq (\log n)^{-1/4}p^{-1}$. For each $v \in V \setminus X$, let Y_v be indicator random variable of the event that $v \in N(X)$. We have $\mathbb{P}(Y_v = 1) = 1 - (1 - p)^{|X|} = (1 + o(1))|X|p$ (the estimate follows from the fact $|X|p = o(1)$). Let $Y = |N(X)| = \sum_{v \in V \setminus X} Y_v$ and note that

$$\mathbb{E}[Y] = \sum_{v \in V \setminus X} \mathbb{P}(Y_v = 1) = (n - |X|)(1 + o(1))|X|p = (1 + o(1))|X|np.$$

Since the events Y_v are mutually independent, we can apply the Chernoff's inequality to get $\mathbb{P}(|Y - \mathbb{E}[Y]| \geq (\varepsilon/2)\mathbb{E}[Y]) \leq e^{-\Omega_\varepsilon(\mathbb{E}[Y])}$. Combine this with the estimate on $\mathbb{E}[Y]$ and we have,

$$\mathbb{P}(Y \leq (1 - \varepsilon)|X|np) \leq e^{-\Omega_\varepsilon(\mathbb{E}[Y])} = e^{-\Omega_\varepsilon(|X|np)},$$

for large enough n . Since $np \geq C \log n$, the probability that $Y = |N(X)| < (1 - \varepsilon)|X|np$ is $e^{-\Omega_\varepsilon(|X|np)} = n^{-C'|X|}$, where $C' = C'(\varepsilon, C)$ can be made arbitrarily large by choosing constant C appropriately.

Taking the union bound over all choices of X , we get

$$\sum_{1 \leq |X| \leq (\log n)^{-1/4} p^{-1}} n^{-C'|X|} \leq \sum_{k=1}^n \binom{n}{k} n^{-C'k} \leq \sum_{k=1}^n \left(\frac{en}{k} \cdot n^{-C'} \right)^k = o(1),$$

which establishes our claim.

(ii) We will first prove that a.a.s. for every pair of disjoint sets X, Y of sizes $n(\log n)^{-1/2} \leq |X| \leq \frac{\varepsilon n}{2}$ and $|Y| \geq (\frac{1}{2} - \frac{3\varepsilon}{2})n$,

$$e_G(X, Y) \geq \left(1 - \frac{\varepsilon}{2}\right) |X||Y|p > \left(\frac{1}{2} - 2\varepsilon\right) |X|np. \quad (1)$$

Indeed, let X, Y be a fixed pair of disjoint sets such that $n(\log n)^{-1/2} \leq |X| \leq \frac{\varepsilon n}{2}$ and $|Y| \geq (\frac{1}{2} - \frac{3\varepsilon}{2})n$. Then $\mathbb{E}[e_G(X, Y)] = |X||Y|p$ and by Chernoff's inequality,

$$\mathbb{P}\left(e_G(X, Y) \leq (1 - \varepsilon/2)|X||Y|p\right) < e^{-\Omega_\varepsilon(|X||Y|p)} \leq e^{-\Omega_\varepsilon(n(\log n)^{1/2})}.$$

Since there are at most 2^{2n} possible choices of the pairs X, Y and the probability above is $\ll 2^{-2n}$, taking the union bound will give our conclusion.

Condition on the event that (1) holds, and assume that there exists a set X of size $n(\log n)^{-1/2} \leq |X| \leq \frac{\varepsilon n}{2}$ which has less than $(\frac{1}{2} + \varepsilon)n$ neighbors in G' . Then there exists a set Y of size at least $|Y| \geq n - (\frac{1}{2} + \varepsilon)n - |X| \geq (\frac{1}{2} - \frac{3\varepsilon}{2})n$ disjoint from X such that there are no edges between X and Y in G' . However, this gives us a contradiction to (1) since

$$0 = e_{G'}(X, Y) \geq e_G(X, Y) - \left(\frac{1}{2} - 2\varepsilon\right) np \cdot |X| > 0.$$

(iii) Condition on the event that (i) and (ii) holds, and assume that G' is not connected. Let X be a set of vertices which induces a connected component in G' , and let $Y = V \setminus X$. By part (i), we know that $|X| \geq (\log n)^{-1/4} p^{-1} \cdot \frac{np}{2} = \frac{1}{2}n(\log n)^{-1/4}$, and then by part (ii), we know that $|X| > \frac{n}{2}$. On the other hand, since Y must also contain a connected component, the same estimate must hold for Y as well. However this cannot happen since the total number of vertices is n . Therefore, G' is connected. \square

3 Rotation and extension

Our main tool in proving Hamiltonicity is Pósa's rotation-extension technique (see [25] and [24, Ch. 10, Problem 20]). We start by briefly discussing this powerful tool which exploits the expansion property of a graph, in order to find long paths and/or cycles.

Let G be a connected graph and let $P = (v_0, \dots, v_\ell)$ be a path on some subset of vertices of G (P is not necessarily a subgraph of G). If $\{v_0, v_\ell\}$ is an edge of G , then we can use it to close P into a cycle. Since G is connected, either the graph $G \cup P$ is Hamiltonian, or there exists a longer path in this graph. In the second case, we say that we *extended* the path P .

Assume that we cannot directly extend P as above, and assume that G contains an edge of the form $\{v_0, v_i\}$ for some i . Then $P' = (v_{i-1}, \dots, v_0, v_i, v_{i+1}, \dots, v_\ell)$ forms another path of length ℓ in $G \cup P$ (see Figure 1). We say that P' is obtained from P by a *rotation* with *fixed endpoint* v_0 , *pivot point* v_i , and *broken edge* $\{v_{i-1}, v_i\}$. Note that after performing this rotation, we can now close a cycle of length ℓ also using the edge $\{v_{i-1}, v_\ell\}$ if it exists in G . As we perform more and more rotations, we will get more such candidate edges (call them *closing edges*). The rotation-extension technique is employed by repeatedly rotating the path until one can find a closing edge in the graph G thereby extending the path.

Let P'' be a path obtained from P by several rounds of rotations. An important observation which we later will use is that for an interval $I = (v_j, \dots, v_k)$ of vertices of P ($0 \leq j < k \leq \ell$), if no edges of I were broken during these rotations, then I appears in P'' either exactly as it does in P , or in the reversed order.

We will use rotations and extension as described above to prove our main theorem. The main technical twist is to split the given graph into two graphs, where the first graph will be used to perform rotations and the second graph to perform extensions. Similar ideas, such as *sprinkling*, has been used in proving many results on Hamiltonicity of random graphs. The one which is closest to our implementation, appears in the recent paper of Ben-Shimon, Krivelevich, and Sudakov [7].

In the following two subsections, we prove that our random graph indeed contains subgraphs which can perform these two roles of rotation and extension. All the graphs that we study from now on are defined over the same vertex set, and we will use this fact without further mentioning.

3.1 Rotation

Definition 3.1. Let δ be a positive constant. We say that a connected graph G on n vertices has property $\mathcal{RE}(\delta)$ if one of the following holds for every path P (not necessarily a subgraph of G): (i) there exists a path longer than P in the graph $G \cup P$, or (ii) there exists a set of vertices S_P of size at least $|S_P| \geq \delta n$ such that for every vertex $v \in S_P$, there exists a set T_v of size $|T_v| \geq \delta n$ such that for every $w \in T_v$, there exists a path of the same length as P in $G \cup P$ over the vertex set $V(P)$ which starts at v and ends at w .

Informally, a graph has property $\mathcal{RE}(\delta)$ if every path is extendable to a longer path, or can be rotated in many different ways. The next lemma, which is the most crucial ingredient of our proof, asserts that we can find a graph with property $\mathcal{RE}(\frac{1}{2} + \varepsilon)$ in random graphs even after deleting some of its edges.

Lemma 3.2. For every positive ε , there exists a constant $C = C(\varepsilon)$ such that for $p \geq \frac{C \log n}{n}$, the random graph $G = G(n, p)$ a.a.s. has the following property: for every graph H of maximum degree at most $(\frac{1}{2} - 2\varepsilon)np$, the graph $G' = G - H$ satisfies $\mathcal{RE}(\frac{1}{2} + \varepsilon)$.

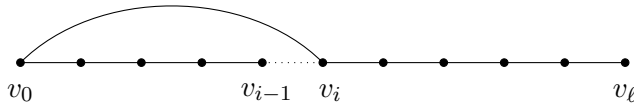


Figure 1: Rotating a path

Proof. Let C be a sufficiently large constant such that the assertions of Propositions 2.3, 2.4, and 2.5 a.a.s. hold, and condition on all of these events. Let H be a subgraph of $G(n, p)$ which has maximum degree at most $(\frac{1}{2} - 2\varepsilon)np$, and let $G' = G - H$. By Proposition 2.3, we know that G' has minimum degree at least $(\frac{1}{2} + \varepsilon)np$, and by Proposition 2.5 (iii), we know that G' is connected. We want to show that $G' \in \mathcal{RE}(\frac{1}{2} + \varepsilon)$ for all choices of H . Consider a path $P = (v_0, \dots, v_\ell)$. If there exists a path longer than P in $G \cup P$, then there is nothing to prove. Thus we may assume that this is not the case. For a set $Z \subseteq V(P)$, let $Z^+ = \{v_{i+1} | v_i \in Z\}$ and $Z^- = \{v_{i-1} | v_i \in Z\}$. For a vertex z , let z^- be the vertex in $\{z\}^-$ and similarly define z^+ .

Step 1 : Initial rotations.

First we show that there exists a set X of linear size such that for all $v \in X$, there exists a path of length ℓ starting at v and ending at v_ℓ . Such X will be constructed iteratively. In the beginning, let $X_0 = \{v_0\}$. Now suppose that we have constructed sets X_i of sizes $4^{-i}(np)^i$ up to some nonnegative i . If $4^{-i}(np)^i \leq \max\{1, (\log n)^{-1/4}p^{-1}\}$, then either by the minimum degree of G' (in case, when $|X_i| = 1$) or by Proposition 2.5 (i), we know that $|N_{G'}(X_i)| \geq (\frac{1}{2} + \varepsilon)|X_i|np$. We must have $N_{G'}(X_i) \subseteq P$ as otherwise we can find a path longer than P . Consequently, we can rotate the endpoints X_i using the vertices in $N_{G'}(X_i)$ as pivot points. If a vertex $w \in N_{G'}(X_i)$ does not belong to any of X_j, X_j^-, X_j^+ for $j < i$, then both edges of the path P incident with w were not broken in the previous rotations. Hence, using w as a pivot point, we get either w^- or w^+ as a new endpoint (see the discussion at the beginning of the section). Therefore, at most two such pivot points can give rise to a same new endpoint, and we obtain a set X_{i+1} of size at least

$$\begin{aligned} |X_{i+1}| &\geq \frac{1}{2} \left(|N_{G'}(X_i)| - 3 \sum_{j=0}^i |X_j| \right) \\ &\geq \frac{1}{2} \left(\left(\frac{1}{2} + \varepsilon \right) \left(\frac{np}{4} \right)^i np - o((np)^{i+1}) \right) \geq \left(\frac{1}{4} \right)^{i+1} (np)^{i+1}, \end{aligned}$$

where $\sum_{j=0}^i |X_j| = o((np)^{i+1})$ since $|X_j| = (np/4)^j$ and $np \geq C \log n$. Repeat the argument above until at step t we have a set of endpoints X_t of size at least $(\log n)^{-1/4}p^{-1}$, and redefine X_t by arbitrarily taking a subset of this set of size $|X_t| = \max\{1, (\log n)^{-1/4}p^{-1}\}$ (note that $t \leq \frac{\log n}{\log(np/4)} \leq \frac{\log n}{\log \log n}$ for $C \geq 4$). Apply the same argument as above to X_t to find a set of endpoints of size at least $\max\left\{\frac{np}{4}, \frac{n}{\log^{1/2} n}\right\}$. Again, if necessary, redefine X_{t+1} to be an arbitrary subset of this set of size $|X_{t+1}| = n/\log^{1/2} n$, and repeat the argument above one more time, now using the second part of Proposition 2.5 instead of the first part to get $|N_{G'}(X_{t+1})| \geq (\frac{1}{2} + \varepsilon)n$. In the end, we obtain a set X_{t+2} of size at least

$$|X_{t+2}| \geq \frac{1}{2} \left(|N_{G'}(X_{t+1})| - 3 \sum_{j=1}^{t+1} |X_j| \right) \geq \frac{n}{4}.$$

Step 2 : Terminal rotation.

Let $X = X_{t+2}$ be the set of size at least $\frac{n}{4}$ that we constructed in Step 1. We will show that another round of rotation gives at least $(\frac{1}{2} + \varepsilon)n$ endpoints. Let Y be the set of all endpoints that we obtain by rotating X one more time (note that Y can contain vertices from X).

Partition the path P into $k = \frac{\log n}{(\log \log n)^{1/2}}$ intervals P_1, \dots, P_k whose lengths are either $\left\lfloor \frac{|P|}{k} \right\rfloor$ or $\left\lceil \frac{|P|}{k} \right\rceil$. Every vertex $w \in X$ was obtained by $t + 2$ rotations which broke $t + 2$ edges of P . If the interval P_i contains none of these edges then the path from w to v_l must traverse P_i exactly in the same order as in P , or in the reverse order (see the discussion at the beginning of the section). Let \hat{X}_i be the collection of vertices of X which were obtained by rotation with some broken edges in P_i . Let $X_{i,+}$ and $X_{i,-}$ be the vertices of X such that P_i is unbroken and paths from these vertices to v_l traverses P_i in the original, and reverse order, respectively. Note that $X = \hat{X}_i \cup X_{i,+} \cup X_{i,-}$ for all i .

The first key fact that we will now verify is that the set \hat{X}_i is small for most indices. Let J be the collection of indices which have $|\hat{X}_i| \geq (\log \log n)^{-1/4} |X|$. Since each vertex in X is obtained by at most $\frac{\log n}{\log \log n} + 2 < 2 \frac{\log n}{\log \log n}$ rotations, we can count the total number of broken edges used for constructing all the points of X in two ways to get

$$|J| \cdot (\log \log n)^{-1/4} |X| \leq |X| \cdot \frac{2 \log n}{\log \log n},$$

which implies $|J| \leq 2 \log n / (\log \log n)^{3/4} = o(k)$.

Our second key fact is that for a vertex $v_j \in P_i$ and a vertex $x \in X_{i,+}$, if $\{x, v_{j+1}\}$ is an edge of G' , then $v_j \in Y$ (similarly, for $x \in X_{i,-}$, if $\{x, v_{j-1}\}$ is an edge of G' , then $v_j \in Y$). Therefore, for all i , there are no edges of G' between $X_{i,+}$ and $(P_i \cap P_i^+) \setminus Y^+$, and between $X_{i,-}$ and $(P_i \cap P_i^-) \setminus Y^-$. We will show that if $|Y| < (\frac{1}{2} + \varepsilon)n$, then this cannot happen because we will have to remove too many edges incident to X from the graph G to form G' .

The number of edges incident to X that we need to remove is at least,

$$e_G(X, V \setminus P) + \sum_{i=1}^k \left(e_G(X_{i,-}, (P_i \cap P_i^-) \setminus Y^-) + e_G(X_{i,+}, (P_i \cap P_i^+) \setminus Y^+) \right).$$

Since $(P_i \cap P_i^-) \setminus Y^-$ and $(P_i \setminus Y)^-$ differs by at most one element (similar for P_i^+), the above expression is

$$e_G(X, V \setminus P) + \sum_{i=1}^k \left(e_G(X_{i,-}, (P_i \setminus Y)^-) + e_G(X_{i,+}, (P_i \setminus Y)^+) + O(|X_{i,-}| + |X_{i,+}|) \right).$$

By definition, $|P_i| = |P|/k = O(\frac{n}{\log n} (\log \log n)^{1/2})$ and $|X_{i,-}| = O(n)$, $|X_{i,+}| = O(n)$. Thus, we can use Proposition 2.4 to get

$$|X| \cdot |V \setminus P| \cdot p + o(n^2 p) + \sum_{i=1}^k \left(|X_{i,-}| \cdot |(P_i \setminus Y)^-| \cdot p + |X_{i,+}| \cdot |(P_i \setminus Y)^+| \cdot p + o\left(\frac{n^2 p}{\log n} \cdot (\log \log n)^{1/2}\right) \right).$$

Since $X = \hat{X}_i \cup X_{i,+} \cup X_{i,-}$ and $||P_i \setminus Y| - |(P_i \setminus Y)^-|| \leq 1$ (also for $(P_i \setminus Y)^+$), this equals to

$$|X| \cdot |V \setminus P| \cdot p + \left(\sum_{i=1}^k |X \setminus \hat{X}_i| \cdot |P_i \setminus Y| \cdot p \right) + o(n^2 p).$$

As observed above, $|X \setminus \hat{X}_i| = (1 - o(1))|X|$ for all but $o(k)$ of indices i , and hence this expression becomes

$$|X| \cdot |V \setminus P| \cdot p + |X|p \cdot \sum_{i=1}^k |P_i \setminus Y| - o(k) \cdot \frac{|P|}{k} |X|p + o(n^2p) = |X| \cdot |V \setminus Y| \cdot p + o(n^2p).$$

On the other hand, this is at most the number of edges incident with X in the graph H which we removed, so it must be less than $|X| \cdot (\frac{1}{2} - 2\varepsilon)np$. Since $|X| \geq n/4$, we must have $|V \setminus Y| \leq (\frac{1}{2} - 2\varepsilon + o(1))n$ and therefore $|Y| \geq (\frac{1}{2} + \varepsilon)n$.

Step 3 : *Rotating the other endpoint.*

In Steps 1 and 2, we constructed a set S_P of size $|S_P| \geq (\frac{1}{2} + \varepsilon)n$ such that for all $v \in S_P$, there exists a path of length ℓ which starts at v and ends at v_ℓ . For each of these paths, we do the same process as in Steps 1 and 2, now keeping v fixed and rotating the other endpoint v_ℓ . In this way we can construct the sets T_v required for the property $\mathcal{RE}(\frac{1}{2} + \varepsilon)$. \square

3.2 Extension

In the previous subsection, we showed that random graphs contain subgraphs which can be used to perform the role of rotations. In this subsection, we show that there exist subgraphs which can perform the role of extensions.

Definition 3.3. Let δ be a positive constant and let G_1 be a graph on n vertices with property $\mathcal{RE}(\delta)$. We say that a graph G_2 *complements* G_1 , if for every path P over the same vertex set as G_1 (P is not necessarily a subgraph of G_1), either there exists a path longer than P in $G_1 \cup P$, or there exist vertices $v \in S_P$ and $w \in T_v$ such that $\{v, w\}$ is an edge of $G_1 \cup G_2$ (the sets S_P and T_v are defined as in Definition 3.1).

Proposition 3.4. *Let δ be a fixed positive constant. For every $G_1 \in \mathcal{RE}(\delta)$ and G_2 complementing G_1 , the union $G_1 \cup G_2$ is Hamiltonian.*

Proof. Let P be the longest path in $G_1 \cup G_2$. By the definition of $\mathcal{RE}(\delta)$, there exists a set S_P such that for all $v \in S_P$, there exists a set T_v such that for all $w \in T_v$, there exists a path of the same length as P which starts at v and ends at w . By the definition of G_2 , there exists $v \in S_P$ and $w \in T_v$ such that $\{v, w\}$ is an edge of $G_1 \cup G_2$. Therefore we have a cycle of length $|P|$ in $G_1 \cup G_2$. Either this cycle is a Hamilton cycle or it is disconnected to the rest of the graph, as otherwise it contradicts the assumption that P is the longest path. However, the latter cannot happen since the graph G_1 is connected by the definition of $\mathcal{RE}(\delta)$. Thus we can conclude that the cycle we found is indeed a Hamilton cycle. \square

The next lemma is the main lemma of this subsection and says that the random graph complements all of its subgraphs with small number of edges.

Lemma 3.5. *For every fixed positive ε , there exist constants $\delta = \delta(\varepsilon)$ and $C = C(\varepsilon)$ such that $G = G(n, p)$ a.a.s. has the following property: for every graph H of maximum degree at most $(\frac{1}{2} - \varepsilon)np$, the graph $G' = G - H$ complements all graphs $R \subseteq G$ which satisfy $\mathcal{RE}(\frac{1}{2} + \varepsilon)$ and have at most δn^2p edges.*

Proof. Let \mathcal{G} be the family of all subgraphs of G obtained by removing at most $(\frac{1}{2} - \varepsilon)np$ edges incident to each vertex. The probability that the assertion of the lemma fails is

$$\begin{aligned} \mathbb{P} &= \mathbb{P}\left(\bigcup_{R \in \mathcal{RE}(\frac{1}{2} + \varepsilon), |E(R)| \leq \delta n^2 p} \left(\{R \subseteq G\} \cap \{\text{some } G' \in \mathcal{G} \text{ does not complement } R\}\right)\right) \\ &\leq \sum_{R \in \mathcal{RE}(\frac{1}{2} + \varepsilon), |E(R)| \leq \delta n^2 p} \mathbb{P}\left(\text{some } G' \in \mathcal{G} \text{ does not complement } R \mid R \subseteq G\right) \cdot \mathbb{P}(R \subseteq G), \end{aligned} \quad (2)$$

where the union (and sum) is taken over all labeled graphs R on n vertices which has property $\mathcal{RE}(\frac{1}{2} + \varepsilon)$ and at most $\delta n^2 p$ edges.

Let us first examine the term $\mathbb{P}(\text{some } G' \in \mathcal{G} \text{ does not complement } R \mid R \subseteq G)$. Let R be a fixed graph with property $\mathcal{RE}(\frac{1}{2} + \varepsilon)$, and P be a fixed path on the same vertex set. The number of such paths is at most $n \cdot n!$, since there are n choices for the length of path P and there are at most $n(n-1)\dots(n-i+1)$ paths of length i , $1 \leq i \leq n$. If in $R \cup P$ there is a path longer than P , then the condition of Definition 3.3 is already satisfied. Therefore we can assume that there is no such path in $R \cup P$. Then, by the definition of property $\mathcal{RE}(\frac{1}{2} + \varepsilon)$, we can find a set S_P and for every $v \in S_P$ a corresponding set T_v , both of size $(\frac{1}{2} + \varepsilon)n$, such that for every $w \in T_v$, there exists a path of the same length as P in $R \cup P$ which starts at v and ends at w . If there exists a vertex $v \in S_P$ and $w \in T_v$ such that $\{v, w\}$ is an edge of R , then this edge is also in $R \cup G'$ (for every $G' \in \mathcal{G}$) and again Definition 3.3 is satisfied. If there are no such edges of R , then since R is a labeled graph, conditioned on $R \subseteq G$, each such pair of vertices is an edge in G independently with probability p . Let S'_P be an arbitrary subset of S_P of size $\frac{\varepsilon}{2}n$, and for each $v \in S'_P$, define T'_v to be the set $T_v \setminus S'_P$. Since $|T'_v| \geq (\frac{1}{2} + \frac{\varepsilon}{2})n$, by Chernoff's inequality, for a fixed vertex $v \in S'_P$, the probability that in $G(n, p)$ this vertex has less than $\frac{1}{2}np$ neighbors in T'_v is at most $e^{-\Omega_\varepsilon(np)}$. Since S'_P is disjoint from all the sets T'_v , these events are independent for different vertices. Thus, using that $|S'_P| = \frac{\varepsilon}{2}n$, we can see that the probability that all vertices $v \in S'_P$ have less than $\frac{1}{2}np$ neighbors in T'_v is at most $e^{-\Omega_\varepsilon(n^2 p)}$.

Note that if some vertex $v \in S'_P$ has at least $\frac{1}{2}np$ neighbors in T'_v , then since every $G' \in \mathcal{G}$ is obtained from G by removing at most $(\frac{1}{2} - \varepsilon)np$ edges from each vertex, there must exist a vertex $w \in T'_v$ such that $\{v, w\}$ is an edge in G' . Therefore if some $G' \in \mathcal{G}$ does not complement the graph R , then a.a.s. there exists some path P such that all vertices $v \in S'_P$ have less than $\frac{1}{2}np$ neighbors in T'_v . Taking the union bound over all choices of path P , we see that for large enough $C = C(\varepsilon)$ and $p \geq \frac{C \log n}{n}$

$$\mathbb{P}(\text{some } G' \text{ does not complement } R \mid R \subseteq G) \leq n \cdot n! \cdot e^{-\Omega_\varepsilon(n^2 p)} = e^{-\Omega_\varepsilon(n^2 p)}.$$

Therefore in (2), the right hand side can be bounded by

$$\mathbb{P} \leq e^{-\Omega_\varepsilon(n^2 p)} \cdot \sum_{R \in \mathcal{RE}(\frac{1}{2} + \varepsilon), |E(R)| \leq \delta n^2 p} \mathbb{P}(R \subseteq G).$$

Also note that for a fixed labeled graph R with k edges $\mathbb{P}(R \subseteq G(n, p)) = p^k$. Therefore, by taking the sum over all possible graphs R with at most $\delta n^2 p$ edges, we can bound the probability that the

assertion of the lemma fails by

$$\mathbb{P} \leq e^{-\Omega_\varepsilon(n^2p)} \sum_{k=1}^{\delta n^2p} \binom{\binom{n}{2}}{k} p^k \leq e^{-\Omega_\varepsilon(n^2p)} \sum_{k=1}^{\delta n^2p} \left(\frac{en^2p}{k}\right)^k.$$

For $\delta \leq 1$, the summand is monotone increasing in the range $1 \leq k \leq \delta n^2p$, and thus we can take the case $k = \delta n^2p$ for an upper bound on every term. This gives

$$\mathbb{P} \leq e^{-\Omega_\varepsilon(n^2p)} \cdot (\delta n^2p) \cdot \left(e\delta^{-1}\right)^{\delta n^2p} = e^{-\Omega_\varepsilon(n^2p)} e^{O(\delta \log(1/\delta)n^2p)},$$

which is $o(1)$ for sufficiently small δ depending on ε . This completes the proof. \square

4 Proof of the main theorem

In this section we prove the main theorem. In view of Lemmas 3.2 and 3.5, we can find both the graphs we need to perform rotations and extensions. However, we cannot immediately apply the two lemmas together, since in order to have valid ‘extensions’ in Lemma 3.5, we need the ‘rotation graph’ to have at most δn^2p edges. Thus to complete the proof, we find a ‘rotation graph’ which has at most δn^2p edges.

Lemma 4.1. *For every positive ε and $\delta < 1$, there exists a constant $C = C(\varepsilon, \delta)$ such that for $p \geq \frac{C \log n}{n}$, the random graph $G(n, p)$ a.a.s. has the following property. For every graph H of maximum degree at most $(\frac{1}{2} - 3\varepsilon)np$, the graph $G' = G(n, p) - H$ contains a subgraph with at most δn^2p edges satisfying $\mathcal{RE}(\frac{1}{2} + \varepsilon)$.*

Proof. Let C' be a sufficiently large constant such that for $p \geq \frac{C' \log n}{n}$, the assertions of Proposition 2.3 and Lemma 3.2 a.a.s. hold, and let $C = C'/\delta$. Let $p' = \delta p$ and let \hat{G} be the graph obtained from $G(n, p)$ by taking every edge of G independently with probability δ . We want to analyze two properties of \hat{G} which together will imply our claim.

Call \hat{G} *good* if it has at most $n^2p' = \delta n^2p$ edges, and all of its subgraphs obtained by removing at most $(\frac{1}{2} - 2\varepsilon)np'$ edges incident to each vertex satisfy $\mathcal{RE}(\frac{1}{2} + \varepsilon)$. Otherwise call it *bad*. Note that by definition, the edge distribution of \hat{G} is identical to that of $G(n, p')$, and therefore by Proposition 2.3 and Lemma 3.2, the probability that \hat{G} is good is $1 - o(1)$. Let \mathcal{P} be the collection of graphs G for which $\mathbb{P}(\hat{G} \text{ is good} \mid G(n, p) = G) \geq \frac{3}{4}$. Since

$$o(1) = \mathbb{P}(\hat{G} \text{ is bad}) \geq \mathbb{P}(G(n, p) \notin \mathcal{P}) \cdot \mathbb{P}(\hat{G} \text{ is bad} \mid G(n, p) \notin \mathcal{P}) \geq \frac{1}{4} \mathbb{P}(G(n, p) \notin \mathcal{P}),$$

we know that $\mathbb{P}(G(n, p) \notin \mathcal{P}) = o(1)$, or in other words, $\mathbb{P}(G(n, p) \in \mathcal{P}) = 1 - o(1)$. Thus from now on, we condition on the event that $G(n, p) \in \mathcal{P}$.

Let H be a graph over the same vertex set as $G(n, p)$ which has maximum degree at most $(\frac{1}{2} - 3\varepsilon)np$. Using the concentration of hypergeometric distribution and taking union bound over all vertices of H , we have that with probability $1 - o(1)$ the graph $\hat{G} \cap H$ has maximum degree at most $(\frac{1}{2} - 2\varepsilon)np'$.

For an arbitrary choice of H , since \hat{G} is good with probability at least $\frac{3}{4}$, and $\hat{G} \cap H$ has maximum degree at most $(\frac{1}{2} - 2\varepsilon)np'$ with probability $1 - o(1)$, there exists a choice of \hat{G} which satisfies these

two properties. For such \hat{G} , by the definition of good, the graph $\hat{G} - H$ satisfies $\mathcal{RE}(\frac{1}{2} + \varepsilon)$. Moreover, \hat{G} has at most $\delta n^2 p$ edges and hence so does $\hat{G} - H$. Since $\hat{G} - H \subseteq G(n, p) - H$, this proves the claim. \square

The main result of the paper easily follows from the facts we have established so far.

Proof of Theorem 1.1. Let δ be sufficiently small and C be sufficiently large constants such that the random graph $G = G(n, p)$ with $p \geq \frac{C \log n}{n}$ a.a.s. satisfies Proposition 2.3 with $\varepsilon/2$ instead of ε , and the assertions of Lemmas 3.5 and 4.1 with $\varepsilon/6$ instead of ε . Condition on these events.

By Proposition 2.3, $G(n, p)$ has maximum degree at most $(1 + \frac{\varepsilon}{2})np$, and thus every subgraph of $G(n, p)$ of minimum degree at least $(\frac{1}{2} + \varepsilon)np$ can be obtained by removing a graph H of maximum degree at most $(\frac{1}{2} - \frac{\varepsilon}{2})np$. Thus it suffices to show that for every graph H on n vertices with maximum degree at most $(\frac{1}{2} - \frac{\varepsilon}{2})np$, the graph $G(n, p) - H$ is Hamiltonian.

Let H be a graph as above. By Lemma 4.1, there exists a subgraph of $G(n, p) - H$ which has at most $\delta n^2 p$ edges and has property $\mathcal{RE}(\frac{1}{2} + \frac{\varepsilon}{6})$. By Lemma 3.5, $G(n, p) - H$ complements this subgraph. Therefore, by Proposition 3.4, $G(n, p) - H$ is Hamiltonian. \square

5 Concluding remarks

In this paper, we proved that when $p \gg \log n/n$, every subgraph of the random graph $G(n, p)$ with minimum degree at least $(1/2 + o(1))np$ is Hamiltonian. This shows that $G(n, p)$ has local resilience $(1/2 + o(1))np$ with respect to Hamiltonicity and positively answers the question of Sudakov and Vu. It would be very interesting to better understand the resilience of random graphs for values of edge probability more close to $\log n/n$, which is a threshold for Hamiltonicity. To formalize this question we need some definitions from [7].

Let $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ be two sequences of n numbers. We write $\mathbf{a} \leq \mathbf{b}$ if $a_i \leq b_i$ for every $1 \leq i \leq n$. Given a labeled graph G on n vertices we denote its degree sequence by $\mathbf{d}_G = (d_1, \dots, d_n)$.

Definition 5.1. Let $G = ([n], E)$ be a graph. Given a sequence $\mathbf{k} = (k_1, \dots, k_n)$ and a monotone increasing graph property \mathcal{P} , we say that G is \mathbf{k} -resilient with respect to the property \mathcal{P} if for every subgraph $H \subseteq G$ such that $\mathbf{d}_H \leq \mathbf{k}$, we have $G - H \in \mathcal{P}$.

It is an intriguing open problem to get a good characterization of sequences \mathbf{k} such the random graph $G(n, p)$ with p close to $\log n/n$ is \mathbf{k} -resilient with respect to Hamiltonicity. Some results in this direction were obtained in [7].

Acknowledgment. We would like to thank Michael Krivelevich for inspiring discussions and conversations. We would also like to thank Alan Frieze and the two anonymous referees for their valuable remarks.

References

- [1] N. Alon and J. Spencer, **The Probabilistic Method**, 2nd ed., Wiley, New York, 2000.

- [2] N. Alon and B. Sudakov, Increasing the chromatic number of a random graph, *Journal of Combinatorics* 1 (2010), 345–356.
- [3] J. Balogh, B. Csaba, and W. Samotij, Local resilience of almost spanning trees in random graphs, *Random Structures and Algorithms* 38 (2011), 121–139.
- [4] J. Balogh, C. Lee, W. Samotij, Corrádi and Hajnal’s theorem for sparse random graphs, *Comb. Probab. Comput.*, DOI:10.1017/S0963548311000642.
- [5] I. Ben-Eliezer, M. Krivelevich and B. Sudakov, Long cycles in subgraphs of (pseudo)random directed graphs, *J. Graph Theory*, to appear.
- [6] S. Ben-Shimon, M. Krivelevich, and B. Sudakov, Local resilience and Hamiltonicity Maker-Breaker games in random-regular graphs, *Combinatorics, Probability, and Computing* 20 (2011), 173–211.
- [7] S. Ben-Shimon, M. Krivelevich, and B. Sudakov, On the resilience of Hamiltonicity and optimal packing of Hamilton cycles in random graphs, *SIAM J. of Discrete Math.* 25 (2011), 1176–1193.
- [8] J. Böttcher, Y. Kohayakawa, and A. Taraz, Almost spanning subgraphs of random graphs after adversarial edge removal, arXiv:1003.0890v1 [math.CO].
- [9] B. Bollobás, Almost all regular graphs are Hamiltonian, *European Journal of Combinatorics*, 4 (1983), 94–106.
- [10] D. Conlon and T. Gowers, Combinatorial theorems relative to a random set, arXiv:1011.4310v1 [math.CO].
- [11] D. Dellamonica, Y. Kohayakawa, M. Marcinişyn, and A. Steger, On the resilience of long cycles in random graphs, *Electron. J. Combin.*, 15 (2008), Research Paper 32.
- [12] G. Dirac, Some theorems on abstract graphs, *Proc. London Math. Soc.*, s3-2 (1952), 69–81.
- [13] A. Frieze and M. Krivelevich, On two Hamiltonian cycle problems in random graphs, *Israel Journal of Mathematics*, 166 (2008), 221–234.
- [14] P. Haxell, Y. Kohayakawa, and T. Łuczak, Turán’s extremal problem in random graphs: forbidding even cycles, *J. Comb. Theory, Ser. B* 64 (1995), 273–287.
- [15] P. Haxell, Y. Kohayakawa, and T. Łuczak, Turán’s extremal problem in random graphs: forbidding odd cycles, *Combinatorica* 16 (1996), 107–122.
- [16] H. Huang, C. Lee, and B. Sudakov, Bandwidth theorem for sparse graphs, *J. Comb. Theory, Ser. B* 102 (2012), 14–37.
- [17] S. Janson, T. Łuczak and A. Ruciński, **Random graphs**, Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience, New York, 2000.

- [18] R. Karp, Reducibility among combinatorial problems, in *Complexity of Computer Computations*, New York: Plenum (1972). 85–103.
- [19] J. Kim, B. Sudakov, and V. Vu, On the asymmetry of random regular graphs and random graphs, *Random Structures and Algorithms* 21 (2002), 216–224.
- [20] J. Komlos and E. Szemerédi, Limit distribution for the existence of Hamilton cycles in random graphs, *Discrete Math.* 43 (1983), 55–63.
- [21] A. Korshunov, Solution of a problem of Erdős and Rényi on Hamilton cycles non-oriented graphs, *Soviet Math. Dokl.*, 17 (1976), 760–764.
- [22] M. Krivelevich, C. Lee, and, B. Sudakov, Resilient pancyclicity of random and pseudorandom graphs, *SIAM J. of Discrete Math.* 24 (2010), 1-16.
- [23] C. Lee and W. Samotij, Pancyclic subgraphs of random graphs, *J. Graph Theory*, DOI:10.1002/jgt.20638.
- [24] L. Lovász, **Combinatorial problems and exercises**, AMS Chelsea Publishing, Providence, RI, 2nd edition, 2007.
- [25] L. Pósa, Hamiltonian circuits in random graphs, *Discrete Math.* 14 (1976), 359–364.
- [26] M. Schacht, Extremal results for random discrete structures, manuscript.
- [27] B. Sudakov and V. Vu, Local resilience of graphs, *Random Structures and Algorithms* 33 (2008), 409-433.